How to decrease the time necessary to run a scan with Fortify

This page has been made public for vendors

Question

My scan with Fortify takes over two hours to complete, how can I make Fortify run faster to decrease the amount of time it takes?

Answer

Beginning with version 4.00, Fortify Static Code Aanalyzer (SCA) supports parallel processing for large projects. If your project scan takes longer than an hour or two to complete, you can dramatically decrease the time necessary to complete the scan by enabling parallel processing. Parallel processing allows you to take advantage of multiple CPUs and cores within a single machine and automatic memory tuning.

Parallel processing allows you to reduce scan times by harnessing the multiple cores, memory, and processing power in your machine. Depending on the nature of your project and your hardware, parallel processing can reduce scan time as much as 90 percent.

While parallel processing can be enabled for all scans, scans that complete in less than 2 hours may not warrant the higher processing power requirements. For this reason, parallel processing is not the default mode of operation. You must enable parallel processing on your system and initiate it on the command line.

Configuring Parallel Analysis Mode

After installing SCA and completing the post-installation steps, you will need to add a couple properties to your SCA configuration file to enable parallel processing.

Add the following properties to your fortify-sca.properties file, located in the <SCA_Installation_Directory>\core\config directory.

Property	Description
com.fortify.sca.RmiWorkerMaxHeap (default: heap size of master JVM)	Sets the heap size for the workers. The amount of memory required varies from project to project, but you don't have to allocate as much memory for the workers as you do for the master JVM. You may need to experiment with this property if you experience low memory warnings, crashes, or don't achieve a significant speed increase. The RmiWorkerMaxHeap property accepts values in kilobytes (K), megabytes (M), or Gigabytes (G). For example, to set the property to 500 kilobytes: -Dcom.fortify.sca.RmiWorkerMaxHeap = 500K
com.fortify.sca.ThreadCount (default: If unchanged, SCA will use all available threads)	You will only need to add this parameter if you need to lower the number of threads used because of a resource constraint. If you experience slow-downs or problems with your scan, reducing the number of threads used may solve the problem.

HPE Fortify Version	4.00 and later
Programming Language	☑ C/C++ ☑ .NET ☑ Java ☑ Objective-C ☑ Other
Fortify Audit Workbench	☑ Yes ☑ No
Fortify IDE Plugin	☑ Yes ☑ No
Other Fortify Component	☑ Yes ☐ No

Request code review tools, validations, and support HERE.

Running in Parallet Analysis Mode

To run source analyzer in parallel analysis mode, add the following parameter to your command string:

```
-j <# worker processes>
```

The ideal number of worker processes is n-2, where n represents the number of processors in your machine. For example, if your machine has 8 processors, the ideal number of worker processes would be 6. There is a single master process that coordinates tasks and the distribution of data to the data workers. Each Java process uses the same amount of memory (unless you overrode it using the com.fortify.sca.RmiWorkerMaxHeapMB in the fortify-sca.properties file). You may need to balance the -Xmx and -j options to insure you don't allocate more memory than is physically available. To figure out the maximum number of workers for your installation:

```
     Total Physical Memory /  (Physical Memory Per Java Process X
Number of processes)
```

Example of translating a single file named MyServlet.java:

```
sourceanalyzer -b MyServlet -cp lib/j2ee.jar MyServlet.java -j 6
```

Additional Information

The Fortify documentation includes a performance guide that provides additional information on tuning the performance of Fortify

References

- HPE Fortify Static Code Analyzer User Guide, Appendix A
- HPE Fortify Static Code Analyzer Performance Guide